Detección de Infraestructuras de Clave Pública anómalas.

Castro Lechtaler, Antonio[1,2] Marcelo Cipriano[1], Eduardo Malvacio[1]

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad de Ingeniería. Instituto Universitario del Ejército.
[2] F.C.E. Universidad de Buenos Aires.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar, edumalvacio@gmail.com

1. Resumen.

Esta línea de investigación busca elaborar un criterio matemático para determinar si una Infraestructura de Clave Pública (PKI de las siglas en inglés de Public Key Infrastructure) se comporta de manera segura y confiable o se detectan anomalías en los certificados emitidos.

Por medio del análisis estadístico de un conjunto de muestras formadas por certificados entregados por la PKI, se determinará si se satisfacen los criterios construidos a partir de propiedades matemáticas y enunciar el comportamiento seguro o inseguro de la misma.

Cabe destacar que un sesgo o una falla en la selección de los valores primos que constituyen a cada certificado, puede provocar debilidades y vulnerabilidades en el control de acceso al sistema, el intercambio de claves para sesiones seguras, problemas con la autenticación de usuarios, mensajes y equipos, etc.

Al determinar las propiedades matemáticas involucradas y la elaboración de los criterios adecuados a la deteccion del comportamiento anormal, se podrá desarrollar un software auditor de PKI.

No se conocen, al día de hoy, fórmulas que generen números primos, ni tampoco se conocen con exactitud la forma en que dichos números se distribuyen. A estos problemas se le suma la dificultad para realizar cálculos precisos con enormes cantidades de dichos números del tamaño que se los emplean en los sistemas actuales.[1]

Palabras Clave:

Seguridad en Redes, Infraestructura de Clave Pública, PKI, Detección de Anomalías, Open-SSL, RSA.

2. Contexto.

El Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CRIPTOLAB) pertenece a la Escuela Superior Técnica “Gral. Div. Manuel N. Savio” (EST), Facultad de Ingeniería, del Instituto Universitario del Ejército Argentino (IUE) en el área del Posgrado en Criptografía y Seguridad Informática que se dicta en esta institución, junto a otros posgrados y carreras de grado en ingeniería.

El desarrollo científico y tecnológico es relevante a nivel estratégico y es por ello que tanto las Fuerzas Armadas en general como el Ejército en particular destina recursos de investigación para cumplir con tal fin.

El Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) realizó aportes a través de Proyectos de Investigación Científico Tecnológicos

[1]Calcular n! con n del orden de 2048 bits, por ejemplo.

Orientados (PICTO) para la realización durante 6 años del proyecto recientemente finalizado sobre "REDES PRIVADAS COMUNITARIAS".

Dentro de dicho proyecto, se llevó adelante gran parte de esta investigación-, cuyos resultados parciales o finales han sido presentados en varios CACIC para su difusión a la comunidad científica.

Sin embargo hemos podido, recién-temente, darle entidad propia a esta línea de investigación al poder incluirla dentro de los proyectos de la EST – IUE bajo el nombre de VULCLAP: Vulnerabilidades en Clave Pública.

Recientemente CITEDEF y el Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación dieron su aval por escrito a este proyecto, dado su interés en ser aplicado en sus propios sistemas y redes.

3. Introducción.

Además de los certificados digitales para autenticar sitios de internet, los sistemas pueden elaborar sus propios certificados para autenticación privada de equipos, usuarios, sesiones, etc. Es por ello que la instalación de una Infraestructura de Clave Pública (PKI) se puede llevar adelante en cualquier sistema que así lo requiera.

Dada la existencia de PKI de código libre y abierto, con licencias de uso gratuitas, es fácil instalar cualquiera de ellas.

¿Cómo comprobar si estos procesos y servicios contienen errores que pueden alterar la seguridad de lo que pretenden proteger? [1].

Hay distintas maneras para analizar el comportamiento anómalo de una PKI. Por ejemplo acceder a su código fuente: revisar las cientos o miles de líneas de programación y analizar así su comportamiento. Dada la complejidad de tal trabajo y la dificultad o imposibilidad de automatizarlo, se ha elegido como alternativa el camino descrito en esta línea de investigación.

La filosofía del código abierto (open source) y la ley de Linux [2] es atractiva desde cierto punto de vista teórico. Pero por sí misma no garantiza la ausencia de errores: por ejemplo bug descubierto por Luciano Bello en OpenSSL2 de Debian. El mismo fue enmendado 20 meses después que la versión defectuosa fuera informada [3]. Y este no es el único ejemplo. Recientemente han sido detectados problemas de seguridad en SSL/TSL en el iOS7 de Apple y GnuTSL de Linux, entre otros.[3]

Se puede detectar el funcionamiento anómalo de una PKI cuando genera un conjunto de números primos sesgados por alguna razón. Así se distancia del comportamiento equiprobable, dentro de ciertos parámetros asumidos, y pasa a tener un comportamiento sesgado. Así, un atacante tiene forma de reconstruir un subconjunto P´ de números primos con los que trabajar y vulnerar la factorización de los módulos públicos y obtener la clave privada de los mismos.

Lenstra y otros [4], han hallado repetición de los números primos en el 5% de una gran muestra de certificados digitales de 1024 bits. Si se repiten los primos, entonces tales certificados son vulnerables.

---

[2] Una mala inicialización de una variable provocó una predictibilidad en el generador de números, abriendo una vulnerabilidad inimaginable.

[3] http://www.securitynull.net/

4. Líneas de Investigación, Desarrollo e Innovación.

Se elaboró una herramienta informática que permite hallar los primos que componen un módulo RSA con la información que aportan su clave pública y su clave privada[5].

Las posteriores pruebas de codificación e implementación demostraron que este procedimiento corría muy veloz[6].

Se comparó el rendimiento del mismo con el procedimiento existente en la bibliografía tradicional para la enseñanza de la criptografía [7].

Los análisis indicaron que la complejidad computacional del algoritmo era del orden O (log n) mientras que el de la bibliografía de referencia tenía un orden O (log3 n) [8].

Se elaboró la herramienta matemática que permitiría detectar anomalías [9].

Se realizó un abordaje probabilístico del problema [10] y por último el diseño final de la herramienta probabilística y estadística [11].

Simultáneamente al avance matemático se ensamblaron y codificaron todas las herramientas matemáticas antes mencionadas, en una plataforma de software programado en C++.

5. Resultados y Objetivos.

Se llevaron adelante pruebas por muestras o lotes: se le solicita a OPEN-SSL la entrega de certificados a efectos de buscar repeticiones o colisiones de primos.

Se han evaluado 80.000.000 de módulos agrupados en 80000 lotes de 1000 cada uno. Los resultados obtenidos siguen sin responder a las predicciones teóricas, Estas dificultades han hecho que se demore el tiempo planteado inicialmente para estas etapas dentro de la línea de investigación.

Se ha hallado que el modelo matemático elegido para la detección de anomalías en la distribución de los primos no fue el adecuado y ya ha sido modificado.

Una vez que se hayan enmendado las líneas de software correspondientes, se simularán diferentes PKI´s con vulnerabilidades y sin ellas. Cada una de ellas en un orden aleatorio, será testeada por el programa. El comportamiento esperado es que detecte las vulnerables e informe al respecto.

Se elaboró una plataforma de computación distribuida a los efectos de acelerar la investigación.

6. Formación de Recursos Humanos.

Desde el año 2012 algunos algoritmos que utilizamos en esta investigación fueron codificados y probados en el contexto de la Cátedra de Computación I a cargo del Ing. Mg. Alejandro Repetto, que posee nuestra facultad en la carrera de Ingeniería Informática.

Desde el año 2013 un equipo de docentes y alumnos del Centro de Investigación y Desarrollo de Software del Ejército Argentino (CIDESO) trabaja en el diseño y elaboración de una plataforma de computación distribuida para que se pueda emplear en problemas de criptología a los que se dedica el Criptolab y se han publicado sus resultados [12].

7. Referencias

[1] Young A and Yung M. *An Elliptic Curve Asymmetric Backdoor in Open-SSL*

RSA Key Generation. Chapter 10. Cryptovirology. 2006.

http://www.cryptovirology.com.

[2] Glass, Robert *"Facts and Fallacies of Software Engineering"*. Addison-Wesley Professional, 2003.

[3] Bello L, Bertacchini M. *"Generador de Números Pseudo-Aleatorios Predecible en Debian"*. III Encuentro Internacional de Seguridad Informática. Manizales, Colombia. Octubre 2009.

[4] Lenstra, A; Hughes, J; Augier, M y otros. Ron was wrong, Whit is right. e-print International Association for Cryptologic Research. 15 Feb 2012

http://eprint.iacr.org/2012/064,

[5] Cipriano, M. "Factorización de N: recuperación de factores primos a partir de las claves pública y privada." XIV Congreso Argentino de Ciencias de la Computación CACIC 2008. Chilecito, La Rioja, Octubre 2008.

[6] Castro Lechtaler, C; Cipriano, M; Benaben A; Quiroga, P. *"Study on the effectiveness and efficiency of an algorithm to factorize N given e and d"*. IX Seminario Iberoamericano en Seguridad de las Tecnologías de la Información, La Habana, CUBA. 2009.

[7] Menezes, A; van Oorschot, P and Vanstone, S. *Handbook of Applied Cryptography*. CRC Press. 5th Edition, 2001.

[8] Benaben, A; Castro Lechtaler, A; Cipriano, M; Foti, A. *"Development, testing and performance evaluation of factoring algorithms whit additional information"* XXVIII Conferencia Internacional de la Sociedad Chilena de Computación. Santiago de Chile. 2009.

[9] Castro Lechtaler, A; Cipriano, M. "*Detección de anomalías en Oráculos tipo OpenSSL por medio del análisis de probabilidades*". XVII Congreso Argentino de Ciencias de la Computación CACIC 2011. La Plata, Buenos Aires, Octubre 2011.

[10] Castro Lechtaler, Antonio, Cipriano Marcelo; Malvacio Eduardo; Cañón, Sebastián; *Procedure for the Detection of Anomalies in Public Key Infrastruture (RSA Systems)*. XIII Simposio Argentino de Tecnología, 41 Jornadas Argentinas de Informática e Investigación Operativa JAIIO – SADIO. La Plata, Buenos Aires, Agosto 2012.

[11] Castro Lechtaler, Antonio; Cipriano, Marcelo; Malvacio, Eduardo. *Experimental detection of anomalies in public key infrastructure*. XVIII Congreso Argentino de Ciencias de la Computación CACIC 2012. Bahía Blanca, Buenos Aires, Octubre 2011.

[12] Castro Lechtaler, A; Repetto, A; Bianchi, O; Cipriano, M; Arroyo Arzubi, A; Cicerchia, C; Malvacio, E. *ULTRACOM: Computación de alto rendimiento para criptoanálisis*. XX Congreso Argentino de Ciencias de la Computación, La Matanza, Buenos Aires, 2014.